AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Rachel S. Corn, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), Baltimore Division, Baltimore, Maryland, being duly sworn, depose and state as follows:

1. I have been a SA with the FBI since May 2006. Since September 2006, I have primarily investigated federal violations concerning child pornography and the sexual exploitation of children. I have gained experience through training in seminars, classes, and daily work related to conducting these types of investigations. Specifically, I have received FBI Crimes Against Children training, FBI Innocent Images Online Undercover training, and FBI Peer-to-Peer Network Online Investigation training. I have participated in the execution of numerous search warrants, of which the majority have involved child exploitation and/or child pornography offenses. Many of the child exploitation and/or child pornography search warrants resulted in the seizure of computers, cell phones, magnetic storage media for computers, other electronic media, and other items evidencing violations of federal laws, including various sections of Title 18, United States Code § 2252A involving child exploitation offenses. I have also participated in the execution of numerous search warrants for online accounts, such as email accounts, online storage accounts and other online communication accounts related to child exploitation and/or child pornography. In the course of my employment with the FBI, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media and within online accounts.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

3. This affidavit is made in support of an application for warrants to search the following (hereinafter referred to as the "TARGET ACCOUNTS"):

a. The Dropbox account associated with the email address seeuuusee@gmail.com and User ID: 457280636 (information specific to this account can be found in paragraphs 30 and 31, below);

b. The Apple account associated with the email address shitmanbaby@gmail.com and DS ID: 8135715294 (information specific to this account can be found in paragraphs 27, 28, and 29, below);

c. The Facebook account associated with the email address ddhman29@gmail.com and User ID: 100004812307628 (information specific to this account can be found in paragraphs 25, 26, and 28c, below);

d. The Instagram accounts associated with the following:

1. geeeasyddh@gmail.com and User ID: 7991022069 (information specific to this account can be found in paragraphs 29, 32, and 34, below);

2. lorpeee@gmail.com and User ID: 25492647686 (information specific to this account can be found in paragraphs 29, 33, and 34, below);

more fully described in Attachments A1, A2, A3, and A4, incorporated by reference.

4. The TARGET ACCOUNTS are to be searched for evidence of violations of Title 18, United States Code, Sections 2251(a) (production of child pornography), Title 18, United States Code, Section 2252A(a)(2) (distribution and receipt of child pornography), Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography), 18 U.S.C. § 2422(b) (Use of Interstate Commerce Facilities to Entice a Minor to Engage in Sexual Activity), and 18 U.S.C. § 2423(b) (Travel With Intent to Engage in Illicit Sexual Conduct) (hereinafter referred to as the "TARGET OFFENSES").

5. The statements in this affidavit are based in part on information and reports provided by NCMEC, Instagram, and Special Agents of the FBI, on my investigation of this matter, and on my experience and background as a Special Agent of the FBI. Since this affidavit

is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of the TARGET OFFENSES are located in the TARGET ACCOUNTS.

SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION, RECEIPT AND DISTRIBUTION OF CHILD PORNOGRAPHY

6. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures,

films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer to Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

7. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The

distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers, smartphones and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers, smartphones and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Mobile devices such as laptop computers, smartphones, iPods, iPads and digital media storage devices are known to be used and stored in vehicles, on persons or other areas outside of the residence.

d. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Many people generally carry their smartphone on their person.

e. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.

f. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

g. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo, and Google, Inc., Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers, and is occasionally retained by the providers after the user deletes the data from their account.

h. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

i. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, there exists a fair probability that evidence regarding the distribution, receipt and possession of child pornography will be found in the TARGET ACCOUNTS notwithstanding the passage of time.

j. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

k. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten.

l. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

m. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 500 GB of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

n. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Since the storage capacity of hard drives has increased dramatically over the last several years, it is more likely that the above-described information will be recovered during forensic analysis.

NCMEC CYBERTIPLINE

8. The National Center for Missing and Exploited Children (NCMEC) receives complaints via their Cybertipline from Internet Service Providers (ISPs), Electronic Service Providers (ESPs), and others. These Cybertipline reports are reviewed by a NCMEC analyst and forwarded to law enforcement for further investigation on the information provided in the Cybertipline report.

DROPBOX

9. Dropbox is a file hosting service that offers "cloud" storage and file synchronization. Dropbox offers free and paid services that allow users to add photos, documents, videos and files to their account. Dropbox makes these files accessible to all of the user's computers and mobile phones, and saves the files to the Dropbox server, so they may be accessed from anywhere. Dropbox offers a free plan that allows users to have 2GB of space to store their files. Dropbox also offers additional space on the Dropbox servers for a fee.

10. According to Dropbox's privacy policy, at https://www.dropbox.com/privacy, Dropbox collects and stores the files users upload and delete and also collects logs. Dropbox records when the user uploads and deletes a file but Dropbox does not record when the user downloads a file. Dropbox collects and associates a user's account with their name, email address, phone number, payment info, physical address, and account activity. Dropbox collects information related to how users use their Services, including actions users take in their account, like sharing, editing, viewing, and moving files or folders. Dropbox also collects information from and about the devices users use to access their Services. This includes things like IP addresses, the type of browser and device used, the web page visited before coming to Dropbox sites, and identifiers associated with the users' devices.

11. In order to create a Dropbox account, a user is required to register with an email address. Once registered, each user is assigned a unique user ID. Dropbox communicates with users via stored email accounts on file when users access and make changes to their accounts unless the user opts-out of those emails. To sign into the user's Dropbox account, the user enters their email and password. Once a user has a Dropbox account, they can invite other Dropbox users to access their shared folders. A shared folder is one in which more than one user has access to, and can add, download or delete content. If a user joins another user's shared folder, the shared folder size counts towards the first user's space limitation. If a user is invited to join another user's folder, the invitation request is sent to the registered email account. A user can share their login information for an account, therefore more than one person could plausibly take actions in the Dropbox account at the same time, but it would all appear as the same user to Dropbox.

12. Dropbox maintains IP addresses for web-based logins and the last-seen IP address of linked computers. IP address information is typically maintained for 6 months. IP addresses of specific actions within a Dropbox account, such as uploads and deletions, are not available. Additionally, if a user is accessing files in their Dropbox account from a desktop or mobile application, that access may not be logged by Dropbox.

13. On January 31, 2018, Dropbox advised that "Dropbox cannot produce content in response to warrants that request any form of account content other than a complete reconstruction of a Dropbox account as it exists on the date of warrant service or a previously served preservation request." Dropbox requires search warrants that do not request them to produce the account for a specific date.

APPLE

14. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). The services include email, instant messaging, and file storage.

15. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

16. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

17. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for Kik, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.

FACEBOOK

18. Facebook is a free social networking website that provides a host of services to its users. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. Facebook users can post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. A particular user's profile page includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links.

19. Facebook has a Photos application, where users can upload images and videos. Another feature of the Photos application is the ability to "tag" (i.e., label) other Facebook users in a photo or video. For Facebook's purposes, a user's "Photoprint" includes all photos uploaded

by that user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

20. Facebook users can exchange private messages with one another. These messages, which are similar to email messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

21. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook also has a Marketplace feature, which allows users to post free classified ads, including items for sale, housing, jobs, and the like.

INSTAGRAM

22. Instagram is an online mobile photo-sharing, video-sharing and social networking service that is available for free. Users create accounts, which allows users to share photos, videos and messages, and control who is able to view their photos, videos and comments. Users can also video chat with one person or a group of people in real time. Instagram is owned by Facebook.

PROBABLE CAUSE

Introduction

23. On September 1, 2020, a grand jury sitting in the District of Maryland returned a two-count indictment charging Gary Rocky Jones ("Jones") with distribution and possession of child pornography. (United States v. Gary Rocky Jones, CCB-20-0283). On September 1, 2020, Jones was arrested and has been detained since that time.

24. Warrants to search each of the TARGET ACCOUNTS were granted prior to Jones' arrest, and the TARGET ACCOUNTS contained evidence of the TARGET OFFENSES. The records from the TARGET ACCOUNTS were provided only through the date of each warrant, which were issued on January 22, 2020, June 19, 2020, and August 12, 2020. Because Jones continued to have control over the TARGET ACCOUNTS, and because those accounts could continue to receive data from other users who were not aware that Jones was arrested, these warrants seeks to search the TARGET ACCOUNTS for records in the accounts after the search warrants were served.

Facebook Account: dhman29@gmail.com and User ID: 100004812307628

25. On January 22, 2020, United States Magistrate Judge J. Mark Coulson, of the District of Maryland, granted search warrants for numerous online accounts in connection to this investigation, including the Facebook account: **ddhman29@gmail.com and User ID: 100004812307628**.

26. A review of the search warrant results provided by Facebook for the account associated with **ddhman29@gmail.com** ("ddhman29") revealed several pictures and videos depicting Gary Rocky Jones. The review also revealed numerous chat conversations in Spanish.

An FBI Analyst translated the Spanish chats. Below is a summary of some of the chats translated in English:

a. On March 30, 2018, ddhman29 engaged in a chat conversation with Other User 1. Other User 1 asked who ddhman29 was and ddhman29 stated, "Someone from the US. I speak English, but I can translate your words with this app." During this conversation ddhman29 said he was 17 years old and Other User 1 said he was 13 years old. During the chat conversation, both users asked to see each other's buttocks. On April 2, 2018, ddhman29 asked Other User 1 "Do you want to see someone young sucking dick?" Ddhman29 sent a video that depicted a prepubescent male's mouth being penetrated by the penis of an adult male.

b. On September 8, 2018, ddhman29 engaged in a chat conversation with Other User 2. In the conversation, Other User 2 sent pictures of his face. On September 13, 2018, Other User 2 sent a picture of his pants unbuttoned and underwear exposed and his hand on what appears to be his clothed penis. Ddhman29 responded, "Let me see." Other User 2 sent a picture of his pants pulled down and underwear exposed. Ddhman29 responded, "Take it out." Other User 2 said, "Really?" and "I'm 15 baby." Ddhman29 responded, "Yes." Other User 2 sent a picture of his exposed erect penis. The background and clothing depicted in this picture is the same from the previous two pictures that Other User 2 sent. Ddhman29 said "Let me see your face and body" and "More." Other User 2 sent additional pictures, including a picture with his face and erect penis depicted. Other User 2 again said, "I'm 15."

c. In a Facebook Marketplace[1] chat, which occurred in English on September 17, 2018, ddhman29 stated to Other User 3, "Put a Ceiling fan in for me." Other User 3 asked "Where?" and ddhman29 responded "4819 Aberdeen ave Baltimore md 21206."

Apple Account: shitmanbaby@gmail.com

27. On January 22, 2020, United States Magistrate Judge J. Mark Coulson, of the District of Maryland, granted search warrants for numerous online accounts in connection to this investigation, including the Apple account: **shitmanbaby@gmail.com and DS ID: 8135715294**.

28. A review of the search warrant results provided by Apple for the account associated with the email address **shitmanbaby@gmail.com** revealed that the primary email address for the account was ddhman2929@icloud.com. The search warrant results revealed more than 4,500

[1] Facebook Marketplace is a digital marketplace where users can arrange to buy, sell and trade items with other people in their area.

images and videos in the Cloud Photo Library and the review of the files is still ongoing. Below is description of some of the files located in the Cloud Photo Library:

a. The image titled "IMG_0094.HEIC" depicted a Maryland Driver's License in the name Gary Rocky Jones, 4819 Aberdeen Avenue, Baltimore, Maryland 21206.

b. The image titled "IMG_0900.HEIC" depicted a document titled, "Sworn Affidavit & Proof of Loss Statement." The document states that it should be completed by the AT&T Account holder. The account holder information is in the name Gary Jones, email address ddhman29@gmail.com, and billing address 4819 Aberdeen Avenue, Baltimore, Maryland 21206 and was signed on June 17, 2019.

c. The video titled "video nov 14, 2 19 27 am.mp4" depicted a prepubescent male whose mouth is being penetrated by the penis of an adult male. This is the same video that was sent by Facebook user **ddhman29** on April 2, 2018, referenced in paragraph 26a. I reviewed the video and concluded, based on my training and experience, that the video contains a visual depiction of a minor engaging in sexually explicit conduct and is child pornography under 18 U.S.C. § 2256(8).

d. The video titled "IMG_0241.mp4" depicted two prepubescent males engaged in oral sex. As the video continues, both prepubescent males have their mouths penetrated by the penis of an adult male. Then one of the prepubescent males turns around and exposes his anus to the camera. I reviewed the video and concluded, based on my training and experience, that the video contains a visual depiction of minors engaging in sexually explicit conduct and is child pornography under 18 U.S.C. § 2256(8).

e. The video titled "8dt.mp4" depicted a prepubescent male whose mouth is being penetrated by the penis of an adult male. As the video continues the adult male penetrates the anus of the prepubescent male with his erect penis. I reviewed the video and concluded, based on my training and experience, that the video contains a visual depiction of minors engaging in sexually explicit conduct and is child pornography under 18 U.S.C. § 2256(8).

f. A video titled "RPReplay_Final1562009378.mp4" depicted a portion of an Instagram chat between two users. One user sent a video to the other user. The video depicted a prepubescent male masturbate and then engage in oral sex with a minor male.

29. The Apple search warrant results also revealed numerous videos in the Cloud Photo Library that appear to be recordings of various real time Instagram video chats and chat messages between various accounts to include **geeeasyddh@gmail.com and User ID: 7991022069** and **lorpeee@gmail.com and User ID: 25492647686**. Within these recordings, the Instagram accounts **geeeasyddh@gmail.com and User ID: 7991022069** and **lorpeee@gmail.com and User**

ID: 25492647686 received images and videos from the other users. Some of these images and videos include depictions of prepubescent and minor males engaged in sexually explicit conduct.

Dropbox Account: **seeuuusee@gmail.com**

30. On June 19, 2020, United States Magistrate Judge Thomas M. DiGirolamo, of the District of Maryland, granted search warrants for numerous online accounts in connection to this investigation, including the Dropbox account: **seeuuusee@gmail.com and User ID: 457280636**.

31. A review of the search warrant results provided by **Dropbox** for the account associated with **seeuuusee@gmail.com**, which is a paid account, revealed numerous folders containing images and videos. One video, titled "video_2017-03-23_00-34-19.mov," was approximately 15 seconds in length and depicted an adult male penetrating the mouth of a prepubescent male with his penis. Another video, titled "2fd78bc2-490d-40f6-b7e8-6d0a0b41fbcb.mp4," was approximately one minute in length and depicted an adult male penetrating the mouth of a prepubescent female with his penis. One image, titled "Photo Jul 11, 8 57 18 PM.jpg," depicted an adult male penetrating the mouth of a prepubescent male with his penis. I reviewed the two videos and one image and concluded, based on my training and experience, that both videos and the one image contain visual depictions of minors engaging in sexually explicit conduct and are child pornography under 18 U.S.C. § 2256(8).

Instagram Accounts:

32. On June 19, 2020, United States Magistrate Judge Thomas M. DiGirolamo, of the District of Maryland, granted search warrants for numerous online accounts in connection to this investigation, including the Instagram account: **geeeasyddh@gmail.com and User ID: 7991022069**.

33. On August 12, 2020, United States Magistrate Judge Thomas M. DiGirolamo, of the District of Maryland, granted search warrants for numerous online accounts in connection to this investigation, including the Instagram account: **lorpeee@gmail.com and User ID: 25492647686**.

34. As mentioned in paragraph 29 above, the Instagram accounts **geeeasyddh@gmail.com and User ID: 7991022069** and **lorpeee@gmail.com and User ID: 25492647686** received images and videos that included depictions of prepubescent and minor males engaged in sexually explicit conduct. A review of the search warrant results provided by Instagram for accounts **geeeasyddh@gmail.com and User ID: 7991022069** and **lorpeee@gmail.com and User ID: 25492647686** revealed chat communications with other users, including chats with minors that were sexual in nature. In some of the chats in account **geeeasyddh@gmail.com and User ID: 7991022069**, images and videos were exchanged, including depictions of minors, at least one is prepubescent, engaged in sexually explicit conduct.

Criminal History and Sex Offender Registration of Gary Rocky Jones

35. In July 2004, Jones was convicted of two counts of Second-Degree Assault in the Circuit Court for Baltimore City. According to the January 2004 police report, two minor males, ages 12 and 14 at the time, disclosed that they were forced to perform oral sex on one another by an adult male they knew as "Man." The abuse occurred at 614 N Lakewood Avenue, Baltimore, Maryland. During the investigation, three other minors were interviewed and stated that while at 614 N Lakewood Avenue, an adult male they know as "Man" showed them a video of one of the minor males performing oral sex on the other minor male. "Man," who resided at 614 Lakewood Avenue, Baltimore, Maryland, was identified as Jones.

36. In 2006, Jones was convicted of two counts of Second-Degree Sex Offense in the Circuit Court for Baltimore City. According to the police report, in October 2005, two minor males, ages 8 and 11, disclosed that on separate occasions, they were paid to perform oral sex on an adult male that they knew as "Man," at 614 N Lakewood Avenue, Baltimore, Maryland. "Man" was later identified as Jones.

37. According to a September 2015 Baltimore City Police report, two officers observed an adult male being chased by a group of juveniles. One juvenile stopped and advised the police officers that the adult male they were chasing had "molested" a minor male. The police officers stopped the adult male that was being chased and identified him as Jones. The minor male, who was 15 years old at the time, was interviewed and disclosed after Jones befriended him, Jones began spending time at the minor male's house. Jones paid the minor male to watch "gay" pornography on Jones' phone. The minor male also disclosed that Jones engaged in anal and oral sex with the minor male and that Jones used his cell phone to record them engaging in oral sex. The charges related to this police report were dismissed.

REQUEST TO EXECUTE WARRANT AT ANY TIME

38. Because the warrant on the TARGET ACCOUNTS will be served on Dropbox, Apple, Facebook and Facebook/Instagram, which will then compile the requested records at a time convenient to each, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

SUMMARY

39. Based on my training and experience, as well as the activity detailed above, I believe that the TARGET ACCOUNTS contained additional evidence of production, distribution,

receipt, and/or possession of child pornography that was saved to the TARGET ACCOUNTS after the search warrants were initially served.

40. Based on the facts detailed above, as well as my training and experience, Gary Rocky Jones appears to have a sexual interest in children that includes communicating about sex with minors that he meets online, soliciting minors to produce and send him images of the minors engaging in sexually explicit conduct; and collecting child pornography. Jones also maintains and controls a large number of accounts for email, online storage and social networking -- under a variety of names, nicknames, and aliases.

41. Based on my training and experience, as well as the activity detailed above, I believe that the user of the TARGET ACCOUNTS is Gary Rocky Jones. I also believe that the user of the TARGET ACCOUNTS (Jones) displays characteristics common to individuals who have a sexual interest in children, and who access with the intent to view and/or, possess, collect, receive, distribute and produce child pornography as discussed in paragraphs 6 and 7 above. Based on these characteristics and because the TARGET ACCOUNTS that are the subject of this affidavit appear to be accessed, controlled, and/or created by the same user (Jones), as well as the facts listed above relating to the use of these accounts, I respectfully submit there is probable cause that TARGET ACCOUNTS (1) contain evidence of production, distribution, receipt, and/or possession of child pornography, and (2) are relevant to determine the ownership and control of the accounts that are linked to the distribution, receipt and/or possession of child pornography. Based on my training and experience, such information may constitute evidence of the TARGET OFFENSES because the information can be used to identify the account's user or users.

42. Warrants to search the TARGET ACCOUNTS were previously granted before JONES' arrest on September 1, 2020. Based on my training and experience, as well as the activity

detailed above, I believe that the TARGET ACCOUNTS contained additional evidence of production, distribution, receipt, and/or possession of child pornography that was saved to the TARGET ACCOUNTS after the search warrants were initially served.

CONCLUSION

43. Based on the foregoing information, I have probable cause to believe that contraband, and evidence, fruits, and instrumentalities of violations of the TARGET OFFENSES as set forth herein and in Attachments B1, B2, B3, and B4, are currently contained in the TARGET ACCOUNTS more fully described in Attachments A1, A2, A3, and A4. I therefore respectfully request that a search warrant be issued authorizing a search of the TARGET ACCOUNTS for the items described above and in Attachments B1, B2, B3, and B4, and authorizing the seizure and examination of any such items found therein.

Rachel S Corn
Special Agent Rachel S. Corn
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. and 41(d)(3) on this 2 day of March, 2021.

Thomas M. DiGirolamo
HONORABLE THOMAS D. DIGIROLAMO
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A1 – Dropbox, Inc.

This warrant applies to information associated with the following Dropbox account:

- The Dropbox account associated with seeuuusee@gmail.com and User ID: 457280636;

that is stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., a business with offices located at 1800 Owens St., Ste. 200 San Francisco, California 94158.

ATTACHMENT A2 – Apple, Inc.

This warrant applies to information associated with the following Apple, Inc. account:

- shitmanbaby@gmail.com and DS ID: 8135715294;

that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., a business with offices located at 1 Infinite Loop, Cupertino, California 95014.

ATTACHMENT A3 – Facebook, Inc.

This warrant applies to information associated with the following Facebook account:

- The Facebook account associated with the email address ddhman29@gmail.com and User ID: 100004812307628;

that is stored at premises owned, maintained, controlled, or operated by Facebook, a social networking company, headquartered at 1601 Willow Road, Menlo Park, California 94025.

ATTACHMENT A4 - Facebook, Inc

This warrant applies to information associated with the following Instagram accounts:

- geeeasyddh@gmail.com and User ID: 7991022069; and
- lorpeee@gmail.com and User ID: 254926476;

that are stored at premises owned, maintained, controlled, or operated by Facebook, a social networking company, headquartered at 1601 Willow Road, Menlo Park, California 94025.

ATTACHMENT B1 – Dropbox, Inc.

I. Files and Accounts to be produced by Dropbox, Inc.

Dropbox shall disclose responsive data, if any, by sending to the Federal Bureau of Investigation, 185 Admiral Cochrane Drive, Suite 101, Annapolis, Maryland 21401, ATTN: Special Agent Rachel Corn, or rscorn@fbi.gov, using UPS or another courier service, or email, notwithstanding 18 U.S.C. 2252A or similar statute or code.

To the extent that the information described in Attachment A1 is within the possession, custody, or control of Dropbox, Inc. including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Dropbox, Inc., Dropbox, Inc**.** is required to disclose the following information to the government for each account or identifier listed in Attachment A1:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, email addresses, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

b. All information automatically recorded by Dropbox, Inc from a user's Device, including its software and all activity using the Services, to include, but not limited to: a utilizing device's IP address, browser type, web page visited immediately prior to connecting to the Dropbox website, all information searched for on the Dropbox website, locale preferences, identification numbers associated with connecting devices, information regarding a user's mobile carrier, and configuration information;

a. The types of services utilized by the user;

b. All files and records or other information stored by an individual using the account, including all images, videos, documents and other files uploaded, downloaded or accessed using the Dropbox service, including all available metadata concerning these files;

e. All records pertaining to communications between Dropbox and any person regarding the account, including contacts with support services and records of actions taken;

f. For each folder within this account, all unredacted records including the unique user ids of each individual who created, joined or utilized the folder, by either adding content or deleting content from the folder;

g. A complete list of all users within each folder found in this account, including every user name, user identification number, corresponding email address, physical address, and date the user joined Dropbox;

h. Records of session times and durations and IP addresses associated with each of these sessions for every user in each folder in this account;

i. Telephone or instrument numbers provided to Dropbox when each of these users created their accounts, and records of all devices connected to the Dropbox accounts for each of the individuals accessing the folders in this account;

j. For each folder found in this account, all information regarding the user who created the folder, the creation date, and a complete listing of all users who joined, accessed, and left the folder, including the dates each joined, accessed or left the folder. All information regarding when, if applicable, each folder was deleted and who deleted it; and

k. For the individuals identified as users of the folders in this account, any means or sources of payment for this service, including credit card and bank account numbers.

II. Information to be seized by Law Enforcement Personnel:

a. Any and all records that relate in any way to the Dropbox, Inc accounts described in Attachment A1 which is evidence, fruits, and instrumentalities of violations of Title 18 U.S.C.§§ 2251(a), 2252A(a)(2), 2252A(a)(5)(B), 2242(b) and 2423(b), specifically that relate to the following:

1. Images, videos and other files depicting the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

2. Communications or documentations regarding the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

3. Communication or documentation regarding access to and/or interaction with minors, to include the enticement of a minor;

4. Records or communication regarding who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;

5. Images depicting the interior or exterior of residences, public establishments, and vehicles;

6. All images, messages and communications, including any and all preparatory steps taken in furtherance of these crimes;

7. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;

8. Evidence of the times the account or identifier listed on Attachment A1 was used;

9. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;

10. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A1 and other associated accounts;

11. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

b. All existing printouts from original storage which concern the categories identified in subsection II.A; and

c. All "address books" or other lists of contacts.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

ATTACHMENT B2 - Apple, Inc.

I. Files and Accounts to be produced by Apple Inc. between January 22, 2020, to the present.

To the extent that the information described in Attachment A2 is within the possession, custody, or control of Apple including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Apple**,** Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A2:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments);

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. The activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used; and

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be Seized by Law Enforcement Personnel

a. Any and all records that relate in any way to the email accounts described in Attachment A2 which is evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2251(a), 2252A(a)(2), 2252A(a)(5)(B), 2242(b) and 2423(b), specifically that relate to the following:

1. Images, videos and other files depicting the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

2. Communications or documentations regarding the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

3. Communication or documentation regarding access to and/or interaction with minors, to include the enticement of a minor;

4. Images depicting the interior or exterior of residences, public establishments, and vehicles;

5. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;

6. Communication, information, documentation and records relating to who created, used, controlled or communicated with the account or identifier, including records about their identities and whereabouts;

7. Evidence of the times the account or identifier listed on Attachment A2 was used;

8. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;

9. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A2 and other associated accounts;

10. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

b. All existing printouts from original storage which concern the categories identified in subsection II.A; and

c. All "address books" or other lists;

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

ATTACHMENT B3 - Facebook, Inc.

I. Files and Accounts to be produced by Facebook between January 22, 2020, to the present.

To the extent that the information described in Attachment A3 is within the possession, custody, or control of Facebook including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Facebook, Facebook is required to disclose the following information to the government for each account or identifier listed in Attachment A3:

a. All contact information, including full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, website, and other personal identifiers of the current status of the profile page and any individuals that have "defriended" them;

b. All Photoprints, including all photos, videos and other files uploaded by the accounts listed in Attachment A3 and all photos, videos and other files uploaded by any user that have the accounts listed in Attachment A3 tagged in them, including all available metadata concerning these files;

c. All Neoprints, including: profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the User's access and use of Facebook applications;

d. All other communications and messages made or received by the user of the accounts listed in Attachment A3, including all private messages and pending "Friend" requests. All photographs, videos and other files sent and received in the private messages;

e. All IP logs, including all records of the IP addresses that logged into the account;

f. All Facebook accounts linked to any of the accounts listed in Attachment A3 which are linked by machine or third-party cookies, email address, IP address, telephone number, or other account-linking methods available to Facebook, and all the previously requested data for the additional accounts linked to the accounts listed in Attachment A3.

g. All information about the User's access and use of Facebook Marketplace;

h. The length of service (including state date), the types of service utilized by the User, and the means and source of any payments associated with the service (including any credit card or bank account number);

i. All privacy settings and other account settings;

j. All records pertaining to communications between Facebook and any person regarding the User or the User's Facebook account, including contacts with support services and records of actions taken;

k. All communication to or from the user/subscriber of the account, including communication regarding the status of the account.

II. Information to be Seized by Law Enforcement Personnel

a. Any and all records that relate in any way to the email accounts described in Attachment A3 which is evidence, fruits, and instrumentalities of violations of Title 18 U.S.C.§§ 2251(a), 2252A(a)(2), 2252A(a)(5)(B), 2242(b) and 2423(b), specifically that relate to the following:

1. Images, videos and other files depicting the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

2. Communications or documentations regarding the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

3. Communication or documentation regarding access to and/or interaction with minors, to include the enticement of a minor;

4. Images depicting the interior or exterior of residences, public establishments, and vehicles;

5. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;

6. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;

7. Evidence of the times the account or identifier listed on Attachment A3 was used;

8. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;

9. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A3 and other associated accounts;

10. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

b. All existing printouts from original storage which concern the categories identified in subsection II.A; and

c. All "address books" or other lists of contact.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

ATTACHMENT B4 - Facebook, Inc.

I. Files and Accounts to be produced by Facebook between June 19, 2020, to the present.

To the extent that the information described in Attachment A4 is within the possession, custody, or control of Facebook including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Facebook, Facebook is required to disclose the following information to the government for each account or identifier listed in Attachment A4:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, email addresses, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

b. All information automatically recorded by Instagram from a user's Device, including its software and all activity using the Services, to include, but not limited to: a utilizing device's IP address, browser type, web page visited immediately prior to connecting to the Instagram website, all information searched for on the Instagram website, locale preferences, identification numbers associated with connecting devices, information regarding a user's mobile carrier, and configuration information;

c. The types of services utilized by the user;

d. All files and records or other information stored by an individual using the account, including all images, videos, documents, communications and other files uploaded, downloaded or accessed using the Instagram service, including all available metadata concerning these files;

e. All records pertaining to communications between Instagram and any person regarding the account, including contacts with support services and records of actions taken;

f. All data and information associated with the personal page and/or profile page, including photographs, videos, audio files, lists of personal interests and preferences, including hashtags;

g. All Instagram accounts linked to any of the accounts listed in Attachment A4 which are linked by machine or third-party cookies, email address, IP address, telephone number, or other account-linking methods available to Instagram, and all the previously requested data for the additional accounts linked to the accounts listed in Attachment A4;

h. A complete list of all users who are followed by the accounts listed in Attachment A4, and a list of all users who are following the accounts listed in Attachment A4, including every user name, user identification number, corresponding email address, physical address, and date the user joined Instagram;

i. All photos, videos, messages and other files to which the accounts in Attachment A4 have been added, tagged, or associated, including any hashtags or captions associated with each photo, a list of all user who "liked" each photo, a list of each user who commented on each photo, and the substance of each comment regarding each photo;

j. All photos, videos, messages and other files posted, screen shot, or stored by the accounts listed in Attachment A4, including any hashtags or captions associated with each photo, a list of all users who "liked" each photo, the usernames of any other user added to or tagged in each photo, a list of each user who commented on each photo, and the substance of any comment regarding each photo;

II. Information to be seized by Law Enforcement Personnel:

Any and all records that relate in any way to the Instagram accounts described in Attachment A4 which is evidence, fruits, and instrumentalities of violations of Title 18 U.S.C.§§ 2251(a), 2252A(a)(2), 2252A(a)(5)(B), 2242(b) and 2423(b), specifically that relate to the following:

1. Images, videos and other files depicting the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

2. Communications or documentations regarding the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

3. Communication or documentation regarding access to and/or interaction with minors, to include the enticement of a minor;

4. Images depicting the interior or exterior of residences, public establishments, and vehicles;

5. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;

6. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;

7. Evidence of the times the account or identifier listed on Attachment A4 was used;

8. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;

9. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A4 and other associated accounts;

10. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

d. All existing printouts from original storage which concern the categories identified in subsection II.A; and

e. All "address books" or other lists of contact.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.